

Techno-economical Viability of Cognitive Solutions for a Factory Scenario

Lieven Tytgat¹, Matthias Barrie², Vânia Gonçalves², Opher Yaron¹, Ingrid Moerman¹, Piet Demeester¹, Sofie Pollin³, Pieter Ballon², Simon Delaere²

¹Department of Information
Technology - IBCN
Ghent University – IBBT
Gaston Crommenlaan 8 (Bus 201),
9050 Gent, Belgium
{firstname.lastname}@intec.ugent.be

²IBBT-SMIT, Vrije Universiteit
Brussel
Pleinlaan 2, 1050 Brussels, Belgium
{firstname.lastname}@vub.ac.be

³IMEC
Kapeldreef 75
3001 Leuven, Belgium
sofie.pollin@imec.be

Abstract— Recent advances in wireless communication theory and semiconductor technology brought wireless to virtually every aspect of our life, and this trend is expected to continue to increase in the future. Unfortunately, as the number of wireless applications grows, the same scarce spectrum is reused over and over again, resulting in increased interference, which jeopardizes the prospect of wireless meeting its high expectations.

Dynamic Spectrum Access proposes to mitigate this problem by adapting the operational parameters of wireless networks to varying interference conditions. However, the involved increase in cost threatens to reduce the benefit of wireless in different environments.

In this paper we examine the economic balance between the added cost and the increased usability brought about by DSA. We focus on a particular real-life scenario – the production floor of an industrial installation – where there is typically extensive utilization of the ISM band. IEEE 802.15.4 wireless sensors monitor production machinery, and IEEE 802.11 WLAN is used as the data backbone. We model the benefit achieved by adding RF sensing technology in terms of reliability and battery lifetime, and qualitatively assess the cost of interference and the potential gain of introducing sensing technology. Based on this techno-economic analysis, we conclude that if implemented correctly, spectrum sensing can bring business gains in real-life applications.

Keywords- sensing, coexistence, dynamic spectrum access networks, business analysis, statistical model, Spectrum Etiquettes for Unlicensed Bands

I. INTRODUCTION

Recent advances in micro- and nano-electronics have enabled the use of wireless communication in virtually every application. As a result, the scarce spectrum is getting crowded with ever more wireless communication devices. It is clear that due to the spectrum bottleneck, more and more new technologies will have to coexist in the same available spectrum bands. This need is very challenging, as it requires increasing levels of spectral efficiency. Indeed, the

coexistence problem is aggravated by the fact that many heterogeneous technologies have to share this scarce spectrum and collaborate to make the most efficient use of it.

Dynamic Spectrum Access (DSA) is a class of mechanisms that aim at improving spectrum sharing. DSA devices are designed to actively cope with interference by adapting their operation characteristics to the dynamic interference environment, in order to avoid either causing interference or being interfered by other networks. In order to achieve this, DSA networks leverage on a variety of cognitive technologies ranging from spectrum sensing (creating awareness about the environment) to agile radios (allowing effective adaptation to the dynamic environment).

When considering actual deployment of DSA in a real-life situation, there is a natural techno-economical tradeoff between benefit and cost. In order to be able to calculate the balance, it is first necessary to quantify the two. It is necessary to estimate the economical benefit that results from the reduced interference, and the added cost that is associated with the implementation and operation of specific DSA techniques.

In this paper we focus on a particular scenario to examine the economic balance between the added cost and the increased usability of DSA. We consider the case of an industrial plant, where an IEEE 802.15.4 based wireless sensor network coexists with an IEEE 802.11 wireless LAN network in the unlicensed ISM band. Throughout the paper we refer to IEEE 802.11 also with the terms WLAN and WiFi, and to IEEE 802.15.4 also with the terms Zigbee and sensor network. Note that IEEE 802.15.4 only defines the physical (PHY) and MAC layers, in contrast to Zigbee that specifies higher layers of communication above IEEE 802.15.4. However, in sake of simplicity we use the three terms (802.15.4, Zigbee and sensor network) to denote the same thing. The sensor network is used to monitor and control the production line, while WLAN is used to provide wireless access to the data network of the plant. It is deployed in the offices and meeting rooms, as well as on the production floor itself – to provide access to machinery

operators that use WLAN equipped handheld devices. Although the common approach is to go to great lengths to avoid interference to the production line control, for example the ISA100.11a industry standard [22], we propose that a more balanced approach is in place. We suggest that the overall economic value of avoiding interference should be considered, calculating the trade-off between the advantages of the lower interference achieved; and the additional cost incurred. Although the WiFi and Zigbee networks are two separate networks that operate independently of each other, we can safely assume that in our scenario they are managed by the same entity, which could mandate all its WiFi and Zigbee network equipment to adhere to some specific requirements, if this makes economical sense. Consequently, this scenario is an excellent test-case for studying the practical benefit of using DSA from a techno-economical point of view.

In this scenario the economical benefit of implementing DSA results from the consequent reduction in machine failure rate and production disruption. This reduction is achieved as a result of improving the reliability of communications of sensor measurements, which brings to faster identification of machine status alerts. The added cost in this case is due to the actual implementation cost of the selected measures, increased maintenance, and increased cost of battery replacement due to shortened battery lifetime.

The coexistence problem in the ISM band has been studied extensively. Petrova et. al. [19] tested experimentally the impact of 802.15.4 on 802.11 by using a Chipcon CC2420EB board. They noted that the interference impact on 802.11b could only be seen when the offset between the central frequencies is minimal (2 MHz) and the 802.11b packet length is larger than 600 bytes. In [20] Muong et. al. evaluate the packet loss rate and throughput for an 802.11b network when interfered with by 802.15.4 traffic. They show that when the distance between the 802.11 receiver and 802.15.4 transmitter is small, performance degradation can be large. In their analysis, however, they assume that the transmissions between networks are independent, which implies that the listen-before-send algorithm for one network does not hear packets from the other network. Neither this assumption nor their analytical results were validated through measurements. In [18] Thonet et al. measure up to 85% Zigbee packet-loss due to 802.11b traffic. In [17] Pollin et al. measure the impact of WiFi on Zigbee and show it is significant. They also show that the Clear Channel Assessment mechanism (CCA) of Zigbee can reduce collisions with WiFi, but is too slow to avoid all WiFi traffic. In [3] Zhen et al. study the 802.11 and 802.15.4 cross-technology CCA and conclude that 802.15.4 is oversensitive to 802.11 signals while 802.11 is insensitive to 802.15.4 signals when they are outside of the Heterogeneous Exclusive CCA Range (HERC) which equals 25m outdoor.

In order to deal with these coexistence problems, various measures for reducing Packet Error Rate (PER) have been proposed, with three main directions taken, namely Time, Frequency and Space based measures. In Space based PER reducing measures, the focus is on spatial reuse of the spectrum. This approach basically boils down to minimizing

the transmit power for a given data rate in order to minimize the collision domain of each transmission. In frequency based measures, the focus is on optimizing the use of the spectral bands, e.g. channel selection algorithms, and multichannel solutions. Finally, time based PER reducing measures try to avoid collisions through intelligent distribution of message transmissions over time.

In this paper we focus on time based PER reduction. In order to avoid collisions, we propose the use of a cross-technology sensing engine (SE) as a CCA agent. This new device is able to detect the presence of one or more signals from different technologies within a given frequency band. We examine two different options for the deployment of sensing engines, and compare them to the reference of not having sensing engines at all. In what follows case 1 is not to use sensing engines at all, case 2 is to use sensing engines only in the Zigbee node, and case 3 is to deploy sensing engines only in the WiFi device.

The remainder of this paper is organized as follows: Section II introduces the specifics of the factory scenario we consider, where multiple heterogeneous networks coexist. In section III we determine the technical advantages and disadvantages for using the sensing engine in the three deployment cases described above. In section IV we evaluate qualitatively the gains achieved by spectrum sensing versus the incurred costs, and conclude that the most promising solution in this scenario is to equip all WiFi nodes with sensing engines. We conclude this paper in section V.

II. SCENARIO

We consider a factory that produces products, and thus generates revenues, by means of an assembly line. A Wireless Sensor Network (WSN) of more than 600 Zigbee sensors is used to monitor machinery and processes. The sensors measure the temperature and other parameters of machinery and processes on the assembly line, and transmit it periodically to a central control and monitoring system. This system alerts human operators in case overheating or other potential malfunction of the machine (which could happen multiple times a day) is observed. A WiFi network is deployed throughout the factory to provide wireless access to the data network of the plant. It consists of a total of 100 devices, including Access Points, wireless terminals and portable devices.

The ZigBee sensor network is interfered by the WiFi network in the factory, as they both operate in the same 2,4 GHz ISM-band [4]. The nature of interference in this scenario is that ZigBee data may be lost during some periods of time, when there are active transmissions of WiFi packets.

If, for example, a machine gets overheated during this period of time, the supervisors will not be alerted in time, which could lead to serious damage to the machine and a full stop of the assembly line. This would have consequences on the production output, with a decrease in revenues as a result. Furthermore, this would also imply additional costs of fixing the machine and re-starting the production line.

The operators of the factory sit in a control room, monitor the status of machinery and act on alarms and

problems. The operators make use of various handheld devices, such as laptops, tablet computers, wireless phones and wireless video cameras. Whenever an operator is moving around the factory or checking the status of the machinery on-the-spot, he can connect to the factory data backbone through the IP-based WiFi network. On every floor of the factory, the operator enjoys the mobility of controlling machinery in loco without losing control of what is happening in the control room and over the processes being managed. Through the laptop or handheld device the operator has access to the control console and can quickly respond to alarms and problems on the factory floor. With the wireless video camera, the operator can share what he sees with the other operators in the control room or with an expert off-site, speeding up the troubleshooting or repair of a problem. Wireless video cameras can also be placed temporarily in the factory floor to observe the behavior of a specific machine.

All the other offices of the factory are also equipped with WiFi connectivity that is used to connect IP phones, laptops and mobile phones, therefore resulting in a large number of networks being detectable at any moment everywhere in the factory.

III. TECHNICAL ANALYSIS

Both Zigbee and WiFi use CCA to sense if the medium is free before transmitting a packet. Although the basic mechanism is identical, the details like bandwidth, sensing time and Rx-Tx turnaround time are technology dependant. In particular, as mentioned in the Introduction, Zigbee CCA typically detects WiFi transmissions, but WiFi CCA does not detect Zigbee transmissions if it is outside the HERC region. We assume we are outside of this region within this paper.

The sensing engine we propose [21] performs cross-technology Clear Channel Assessment. It can be tuned very quickly to any channel in the ISM band, and then detect any Zigbee or WiFi transmission. Thus, if it is implemented on a Zigbee node, it can also detect WiFi transmissions, and if it is implemented in a WiFi device, it can also detect all Zigbee transmissions across the full WiFi channel. In addition, since it uses dedicated hardware, it helps reducing the Rx-Tx turnaround time significantly.

We examine the three different deployment cases described above, and focus on the consequences to the Zigbee network. We do not consider the impact on the WiFi network, as it is not part of any closed control loop, and therefore does not directly influence the operation of machines.

A. Packet Error Rate

In the analysis that follows we make the following assumptions.

1. The Zigbee network is designed as a single-hop topology, i.e. every sensor is within range of the sink to which it sends its data.
2. The background transmissions of WiFi and Zigbee are independent.

3. All packet lengths and inter packet delays (IPD) are distributed exponentially. This is a simplifying assumption that is made to make probability calculations easy. It is partially justified by the fact that we look at aggregated traffic, as opposed to traffic generated by single nodes. Indeed, specific nodes may create bursty traffic, e.g. during file transfers, or periodic traffic, e.g. during VoIP calls, which are not at all exponential. However, the combination of a large number of nodes with different traffic processes can be expected to be much more ‘well behaved’ than any of its constituents. It is left for further research to study experimentally the nature of aggregated traffic in WLAN and WSN, and the extent to which the ‘distance’ from exponential distribution affects the results presented below.
4. The average length of Zigbee packets is 30 bytes.
5. The average length of WiFi packets is 1250 bytes.
6. The average of the random backoff interval of Zigbee is large compared to the average packet length and inter-packet delay of WiFi.
7. If a Zigbee transmission collides with a WiFi transmission, then the Zigbee packet is lost.
8. Every WiFi packet lasts longer than the Zigbee CCA + Rx-Tx turnaround time.
9. In order for Zigbee CCA to sense a busy channel, the channel must be busy during the complete CCA period.
10. Zigbee CCA senses WiFi transmissions.
11. WiFi CCA does not sense Zigbee transmissions.
12. The sensing engine is ideal – it has no sensing errors (missed packets or false alarms), the sensing time is negligible, and the Rx-Tx turnaround time is reduced to zero (as the sensing engine uses dedicated hardware.)

The terminology we use in the analysis is as follows:

$errZ$:= The event of a Zigbee packet being lost

PER :=

Average Packet Error Rate in the Zigbee network

By definition $PER = E(errZ)$

PER_Z := PER given only Zigbee interference (standalone zigbee network)

We assume that the standalone Zigbee network is designed to be reliable, resulting in a very low PER_Z

W := The event of WiFi being active (transmitting)

\bar{W} := The event of WiFi being not active

T_W := The average WiFi packet length

$T_{\bar{W}}$:= The average WiFi inter packet delay (IPD)

Z := The event of Zigbee being active (transmitting)

\bar{Z} := The event of Zigbee being not active

T_Z

:= The average Zigbee packet length, including CCA and Rx → Tx turnaround

T_{Z0} := CCA time + Rx → Tx turnaround time

$T_{\bar{Z}}$:= The average Zigbee inter packet delay (IPD)

Every WiFi packet transmission starting during Zigbee CCA or Rx-Tx turnaround will result in the Zigbee packet being lost, as we assume that every WiFi packet is longer than this time.

$\delta :=$ Duty cycle

$Z_0 :=$ The moment Zigbee starts CCA

1) Case 1: No sensing engines

The total PER can be separated into the case where WiFi is active (transmitting) at the moment Zigbee starts CCA (denoted $W(Z_0)$), and the case where WiFi is not active at the moment Zigbee starts CCA (denoted $\bar{W}(Z_0)$).

$$PER = E(errZ) = E(errZ|W(Z_0)) * Pr(W(Z_0)) + E(errZ|\bar{W}(Z_0)) * Pr(\bar{W}(Z_0)) \quad (1)$$

If WiFi is transmitting at Z_0 , Zigbee CCA will sense it and initiate a random backoff. Since we assume the average backoff is large compared to T_W and $T_{\bar{W}}$, this can be seen as an independent transmission of the same packet. Thus:

$$E(errZ|W(Z_0)) = E(errZ) = PER \quad (2)$$

Furthermore, the probability of WiFi being active at the moment Zigbee starts CCA equals the duty cycle of WiFi.

$$Pr(W(Z_0)) = Pr(W) = \delta_w \quad (3)$$

$$Pr(\bar{W}(Z_0)) = 1 - Pr(W(Z_0)) = 1 - \delta_w \quad (4)$$

The remaining factor of (1) can be separated into the case where WiFi starts transmitting during the Zigbee transmission, and the case where WiFi does not start transmitting during the Zigbee transmission.

$$\begin{aligned} E(errZ|\bar{W}(Z_0)) = & E(errZ|\bar{W}(Z_0) \cap \{W \text{ starts during } Z\}) \\ & * Pr(W \text{ starts during } Z|\bar{W}(Z_0)) \\ & + (errZ|\bar{W}(Z_0) \cap \{\bar{W} \text{ starts during } Z\}) \\ & * Pr(\bar{W} \text{ starts during } Z|\bar{W}(Z_0)) \end{aligned} \quad (5)$$

The event $\bar{W}(Z_0)$ means that there is no WiFi transmission when Zigbee starts CCA, and therefore Zigbee will start transmitting. If WiFi starts transmitting during the Zigbee packet, we assume the packet is lost. Therefore

$$E(errZ|\bar{W}(Z_0) \cap \{W \text{ starts during } Z\}) = 1 \quad (6)$$

The probability of WiFi starting to transmit during the Zigbee packet, given it did not transmit at Z_0 , equals the probability of an exponential random variable with average $T_{\bar{W}}$ being smaller than the *length* of the Zigbee packet, which we approximate by the probability of this random variable being smaller than the *average length* of the Zigbee packet, T_Z . Therefore:

$$Pr(W \text{ starts during } Z|\bar{W}(Z_0)) \cong 1 - e^{-\frac{T_Z}{T_{\bar{W}}}} \quad (7)$$

If WiFi does not start transmitting during the Zigbee packet, then errors occur according to stand-alone Zigbee. Therefore

$$E(errZ|\bar{W}(Z_0) \cap \{\bar{W} \text{ starts during } Z\}) = PER_Z \quad (8)$$

And the probability of this happening equals:

$$Pr(\bar{W} \text{ starts during } Z|\bar{W}(Z_0)) \cong e^{-\frac{T_Z}{T_{\bar{W}}}} \quad (9)$$

Substituting (6), (7), (8) and (9) into (5), and (2), (3), (4) and (5) into (1) gives us:

$$\begin{aligned} PER = & PER * \delta_w \\ & + (1 - \delta_w) * \left(1 - e^{-\frac{T_Z}{T_{\bar{W}}}} + PER_Z * e^{-\frac{T_Z}{T_{\bar{W}}}} \right) \end{aligned}$$

Solving for PER we get

$$PER = 1 - e^{-\frac{T_Z}{T_{\bar{W}}}} (1 - PER_Z) \quad (10)$$

Or, by replacing error rate with success rate:

$$PSR = 1 - PER; PSR_Z = 1 - PER_Z \quad (11)$$

We get

$$PSR = e^{-\frac{T_Z}{T_{\bar{W}}}} * PSR_Z \quad (12)$$

One simple (and intuitive) consequence of this formula is that the Packet Success Rate (PSR) of Zigbee in presence of WiFi is always lower than the PSR of Zigbee without the presence of WiFi. In other words, the PER of Zigbee in presence of WiFi is always higher than the PER of Zigbee without the presence of WiFi. Fig. 1 shows a plot of the PER of the Zigbee network as a function of the load on the WiFi network for different WiFi data rates.

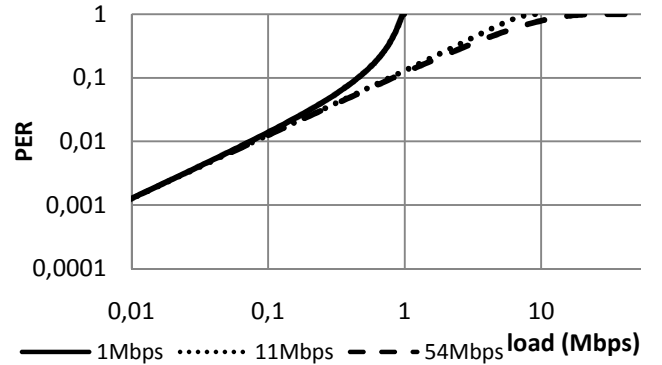


Figure 1. Zigbee PER as function of WiFi load and datarate – no deployment of sensing engine

2) Case 2: Sensing engine on Zigbee nodes

When adding sensing engines to the Zigbee nodes, they allow Zigbee to detect interference faster. Since we assume Zigbee CCA detects WiFi packets, the only impact of introducing an ideal sensing engine is the reduction of T_{Z_0} to zero, which in our terminology translates to reducing T_Z by T_{Z_0} . From (12) we get,

$$PSR = e^{-\frac{T_Z - T_{Z_0}}{T_{\bar{W}}}} * PSR_Z \quad (13)$$

For Zigbee $T_{Z_0} = 304\mu s$, and the largest packet lasts 4ms, thus only a small improvement in PER can be expected in the general case. However, in our scenario we assume

average packet length of 30 bytes, or around 1ms, which makes the reduction in PER a little more significant. Fig. 2 shows a plot of the PER of the Zigbee network as a function of the load on the WiFi network for different WiFi data rates.

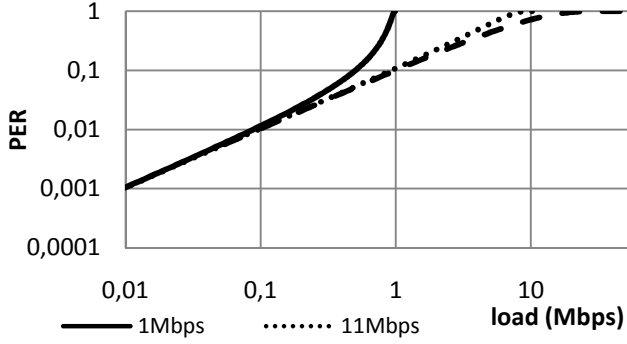


Figure 2. Zigbee PER as function of WiFi load and datarate – sensing engine deployed in Zigbee sensors

3) Case 3: Sensing engine on WiFi nodes

When adding sensing engines to the WiFi nodes, they allow WiFi to detect Zigbee transmissions. Consequently, if there is no WiFi transmission at Z_0 then it can only start during the CCA + Rx-Tx turn around, during which there is still no Zigbee transmission. As soon as Zigbee starts to transit, the sensing engine on the WiFi nodes will detect it, and no WiFi transmission will start. Consequently, (7) and (9) need to be modified. We get

$$Pr(W \text{ starts during } Z|\bar{W}(Z_0)) = e^{-\frac{T_{Z0}}{T_W}} \quad (14)$$

$$Pr(\bar{W} \text{ starts during } Z|\bar{W}(Z_0)) = 1 - e^{-\frac{T_{Z0}}{T_W}} \quad (15)$$

Substituting (6), (14), (8) and (15) into (5), and (2), (3), (4) and (5) into (1) gives us:

$$PER = 1 - e^{-\frac{T_{Z0}}{T_W}(1 - PER_Z)} \quad (16)$$

Or, by replacing error rate with success rate:

$$PSR = e^{-\frac{T_{Z0}}{T_W} * PSR_Z} \quad (17)$$

Fig. 3 shows a plot of the PER of the Zigbee network as a function of the load on the WiFi network for different WiFi data rates. It presents an improvement by a factor of 3 for WiFi loads of up to approximately 20%.

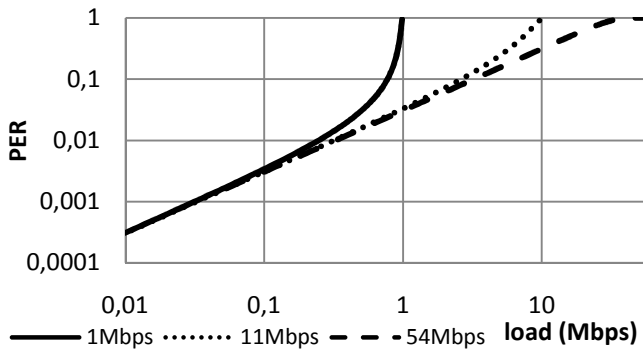


Figure 3. Zigbee PER as function of WiFi load and datarate – sensing engine deployed in WiFi nodes

B. Reliability

A classification of industrial control and monitoring systems is given in [16]. For control applications, the acceptable latency typically ranges between tens of milliseconds and seconds, with required reliability of nine 9s, i.e. 99.999999%. We define Reliability Error Rate (RER) to be the probability of failing to deliver a message within the specified acceptable latency. Using this terminology, control applications require RER of 10^{-9} within the acceptable latency.

RER can be improved by means of packet retransmissions, at the cost of increasing latency. For this purpose a variety of well-known Link-Layer protocols can be used, e.g. Automatic Repeat reQuest (ARQ). In order to determine RER, we calculate the number of retransmissions possible within a given latency requirement. Typical total transmit latency and retransmit timeout are 5ms. Fig. 4 shows the achievable RER as a function of PER for different values of acceptable latency.

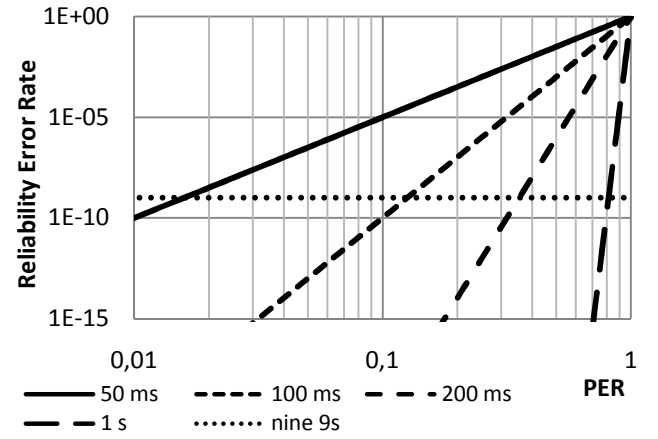


Figure 4. Achievable RER as function of acceptable latency and PER

For example, assume a sensing engine is deployed in the WiFi nodes, and the factory uses a 54 Mbps WiFi network (IEEE 802.11g). If the required RER is 10^{-9} within latency of 200 ms, then we get from Fig. 4 that the Zigbee PER can be as high as ~0.35. Now looking at Fig. 3, we see that Zigbee PER of 0.35 corresponds to WiFi load of ~10 Mbps.

Fig. 5 shows the minimum latency to achieve an RER of nine 9s as a function of WiFi load, for WiFi network of 54 Mbps.

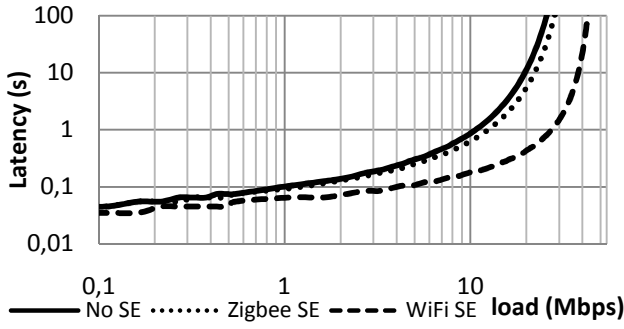


Figure 5. Latency for RER of nine 9s with WiFi of 54Mbps

C. Node lifetime

Within WSNs, the power consumption of the sensor nodes is crucial, as in many cases they are powered by batteries. As demonstrated above, RER can be improved by retransmissions. However, retransmissions consume additional energy, and thus reduce node lifetime. The average number of retransmissions that are needed for successful message delivery depends exclusively on PER. We assume that the radio is the major power consumer, and it is awake during transmission, retransmission and processing time described in III.B. In cases 1 and 3 sensing engines are not deployed at the Zigbee nodes. Typical consumption of the radio in this case, when awake, is 40 mW. In Case 2 sensing engines are added to the Zigbee nodes. The sensing engine needs to be awake during CCA, at which time it consumes 112 mW [21]. The reduction factor in lifetime in these two cases is depicted in Fig. 5.

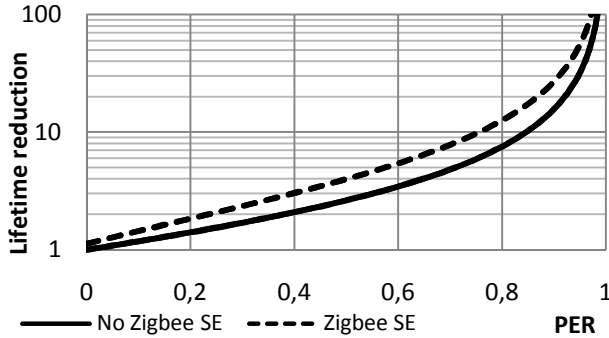


Figure 6. Lifetime Reduction due to Packet Retransmissions

Continuing the example from the previous section, Zigbee PER is ~ 0.35 , which according to Fig. 6 results in lifetime reduction of ~ 2 , or 50%, relative to Zigbee nodes that do not perform retransmissions.

As a final step, we combine the lifetime reduction dependency of Fig. 6 with the calculated PER for the three Cases, for the case of WiFi network of 54 Mbps. The result is depicted in Fig. 7.

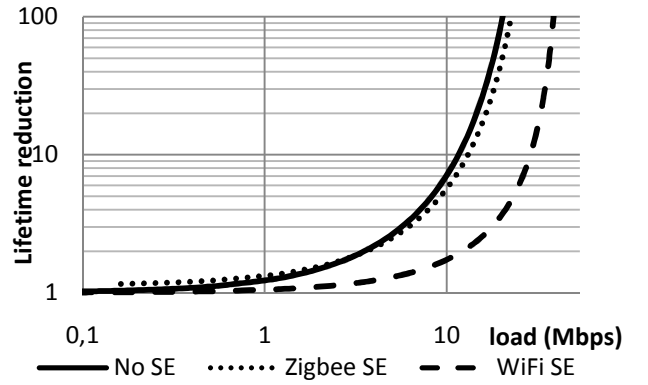


Figure 7. Lifetime reduction in different Cases

Case 2 (Zigbee based sensing engine) consumes most energy for WiFi loads below 3 Mbps due to the increased power consumption of the sensing engine. Above 3 Mbps Case 1 (no sensing engine) consumes most energy due to more packet retransmissions. Case 3 (WiFi base sensing engine) consumes ~ 3 times less than the other cases at a WiFi load of 10 Mbps.

D. Conclusions

Our technical analysis reveals that from the perspectives of the two important aspects of reliability and node lifetime, deploying sensing engines at the Zigbee nodes result in minimal benefits, but deploying them at the WiFi nodes result in substantial improvement. As a concluding example, we compare in Table II the different deployment cases with respect to allowable WiFi load at 54 Mbps for these two different aspects. Specifically, we compare the allowable load in order to stay below a latency of 1s with an RER of $1E-9$, and the allowable load in order to limit the lifetime reduction to a maximum factor of 10.

TABLE I. COMPARISON OF THE DEPLOYMENT CASES

deployment case	Allowable WiFi load for 1s latency	Allowable WiFi load for lifetime / 10
No SE	10,8 Mbps	11,9 Mbps
Zigbee SE	13 Mbps	13 Mbps
WiFi SE	27,5 Mbps	29,2 Mbps

The difference between “no SE” (Case 1) and “Zigbee SE” (Case 2) is only 2,2 Mbps for latency and 1,1 Mbps for lifetime reduction.

In contrast, “WiFi SE” (Case 3) allows a substantial increase in WiFi load of 16,7 Mbps for latency and 17,3 Mbps for lifetime reduction.

IV. BUSINESS ANALYSIS

A. Introduction

One condition for a technology to be adopted is that there should be substantial gains. Therefore, in order to conduct a business analysis of a technology we would need to look at the balance between economical gains and costs of the

technology. This is not only true for specific cognitive radio technologies, but also for wireless technology in general. Therefore, we will first discuss the main drivers for switching from wired to wireless networks, before looking into the business analysis of a specific industrial setting in which cognitive elements are introduced. The focus in this paper is on qualitative analysis of the gains and costs involved with introducing sensing technology. The aim is to firstly evaluate the potential value of such solutions, and to identify the necessary elements for quantitative analysis, which is left for future research.

The benefits of having wireless networks in a factory setting are clear: there is no need for wires throughout the factory, and mobile connectivity for factory employees becomes possible. A first benefit of wireless networks that is often mentioned comes down to cost savings [1][5][6][7]. These savings are made possible by removing the cost of wiring and multiple stationary devices, such as desktop computers. A second advantage is the increased usability of wireless networks as they provide the users with easier access [14] and easier setup [2] of the network. A third category of benefits entails the increased flexibility, reconfigurability and scalability of the network [2][9].

However, the implementation of new technologies always brings additional costs and issues. Often, innovative technology is quite expensive in early stages when brought to the market [1], although in most cases, the purchase of the technology could be looked at as an investment which could lead to significant cost savings. Another challenge, which could prevent straightforward deployment of wireless technologies, is the mere fact that lower data rates are typically achieved [9]. This hampers the use of wireless for high demanding applications, such as HD television.

Battery lifetime and energy consumption is another consideration that network owners should take into account when dealing with radio interfaces. It goes without saying that the energy cost and the battery replacement costs should not be underestimated. Nonetheless, different wireless technologies have different battery life, ranging from 0,5 days (in extreme conditions for WLAN IEEE 802.11a/b/g) to over 1000 days (in good conditions for Zigbee IEEE 802.15.4), so it is up to the network owner to find the appropriate balance between power consumption and capabilities of its network [14].

Furthermore, one of the most important challenges for wireless technologies is reliability [8][10]. Wireless transmissions should take into account some degree of packet loss, especially when coexistence with other wireless systems may lead to harmful interference. In an ideal situation, every packet would follow its trajectory and arrive at the destination without loss. However, multiple factors like variable transmitting power, multi-hop transmission, noise and interference make it impossible to avoid any packet loss. Up to some level of packet loss, the resulting reliability is still acceptable. Therefore it is of utmost importance for wireless technologies to reduce packet loss as much as possible, in order to achieve acceptable reliability.

Cognitive radio networks could play an important role to solve these issues since they are by design more tolerant to interference and coexistence problems. By using cognitive radio, interference between multiple wireless signals can be reduced by means of context awareness, and dynamic spectrum access and channel selection, based on local spectrum occupancy. This way, reliability of wireless networks would increase since packet loss caused by interference would be limited. One technique in obtaining such real-time information about spectrum occupancy is spectrum sensing. However, like any other wireless technology, the implementation of spectrum sensing engines into wireless nodes also implies additional costs, and reduced battery life of the node due to increased power consumption. It is clear that the economical benefits of implementing spectrum sensing should outweigh these costs in order to make sensing economically viable.

In order to draw conclusions on the economical viability of cognitive solutions, such as spectrum sensing, we therefore need to model the gains of the technology versus the incurred costs. To do so, we propose to analyze qualitatively a hypothetical scenario (described in chapter 1) which considers the implementation of spectrum sensing in a factory setting.

B. Analysis

We study the particular scenario of a factory setting in which a WiFi network is used for wireless data connectivity and a Zigbee sensor network is used for monitoring and control of production machinery. Both these networks operate in the same 2,4GHz ISM-band, leading to increased interference between the two technologies. Therefore, in this particular case and as shown in the technical analysis section, the impact of interference could be limited by using Zigbee nodes or WiFi devices that are equipped with spectrum sensing engines. Implementing a solution with spectrum sensing functionalities will however require additional costs, e.g. purchase, implementation, maintenance and power consumption. In order to conclude that cognitive solutions, such as spectrum sensing, are viable, we would therefore need to investigate whether it is worthwhile from an economic perspective to invest in such a technology.

To do so, we start with a qualitative model of the trade-off between the increased reliability of the networks involved and the additional costs in this specific case study. We compare the reference case (no sensing engines deployed) to the two alternatives (sensing engines deployed in respectively Zigbee and WiFi devices). Hence, spectrum sensing technology would be viable in a factory setting if the economical benefit derived from the technology outweighs the additional costs. The implementation of spectrum sensing would then result in profit for the factory.

Our first step is to look at the energy cost of the wireless networks in each of the cases. In this scenario the Zigbee sensors are typically powered by batteries, which need to be replaced when depleted – this is a high cost maintenance operation that may involve complete shutdown of production. The WiFi nodes are powered either by mains power or rechargeable batteries, and do not generate

additional cost beyond the actual cost of consumed electricity. Consequently, the energy cost is composed of 3 components: (i) the cost of Zigbee batteries; (ii) the cost of replacing Zigbee batteries; and (iii) the cost of electrical power consumed by the WiFi nodes.

In case 1 no sensing engines are installed and thus no additional energy cost exists. In case 2 sensing engines are introduced in the 600 Zigbee nodes throughout the factory. Based on the technical analysis, we conclude that this has no effect on the WiFi energy cost, while Zigbee benefits a small energy gain due to the slight decrease in PER and consequent retransmissions. However, as the sensing engines' sensitivity rises (to increase reliability), the extra energy consumption might not be adequately compensated by this increased efficiency, and thus the costs will rise again. Fig. 8 illustrates this qualitative analysis graphically. It shows that the total energy cost (the sum of Zigbee and WiFi costs) of case 2 is lower than that of case 1, which equals the total energy cost before introducing spectrum sensing. If, however, the sensing engines need to be more reliable, their energy costs will grow, and will likely outgrow the moderate improvement in PER.

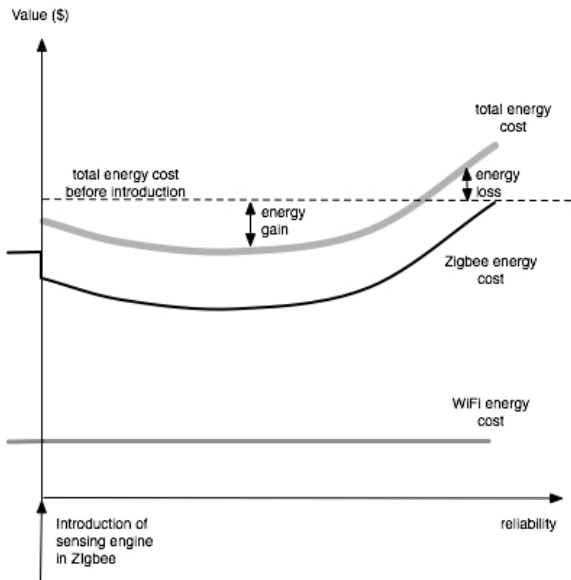


Figure 8. Case 2 – Energy gains

In case 3 sensing engines are introduced in the 100 WiFi devices used throughout the factory, but not in the Zigbee nodes. This increases the costs of WiFi energy consumption rather significantly. However, as shown by the technical analysis, Zigbee nodes would benefit a dramatic decrease in PER and consequent energy-consuming retransmissions, resulting in significant energy cost savings. In this case it is much more likely that even if the sensing engines need to be more reliable, and consume more energy, their energy costs will still be offset by the significant improvement in Zigbee PER. Fig. 9 illustrates this qualitative analysis graphically.

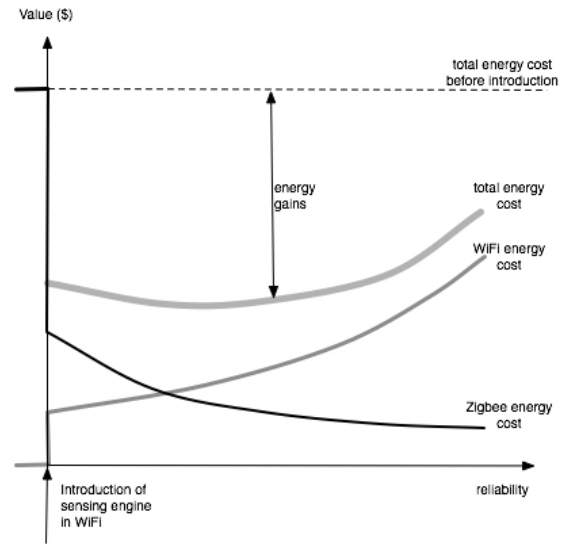


Figure 9. Case 3 – Energy gains

Energy costs are not the only expenditures that should be taken into account by factory owners. Implementing sensing engines in wireless networks also requires a fixed investment. In case 2 this investment is higher than in case 3 due to two factors. First, there is a larger number of Zigbee nodes in the scenario considered (600), compared to only 100 WiFi devices. Secondly, the cost of each sensing engine for WiFi is lower than that for Zigbee, since WiFi devices contain some components that can be reused by the sensing engine while this cannot be done for Zigbee sensors.

By taking the sum of the fixed investment and the total energy costs, the total costs can now be derived. It is obvious that these will be higher in case 2 (Fig. 10) than in case 3 (Fig. 11), due to the higher investment and the higher energy costs.

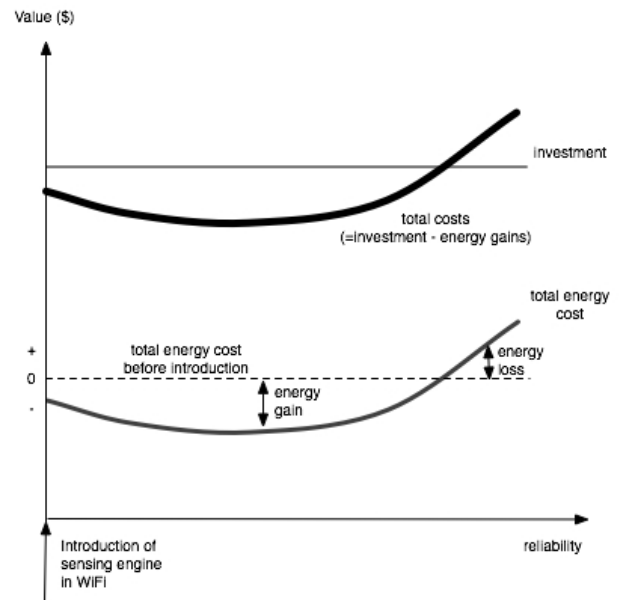


Figure 10. Case 2 – Total Cost

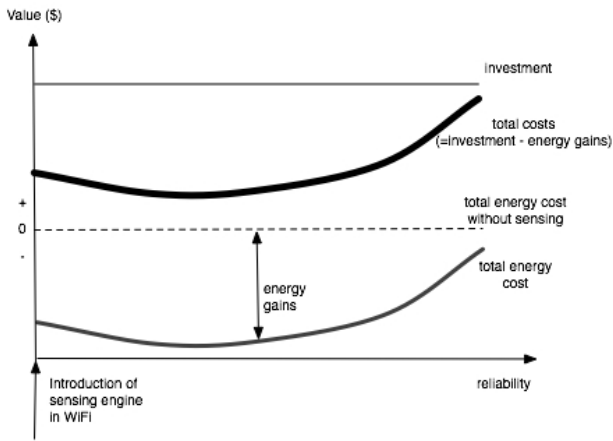


Figure 11. Case 3 – Total Cost

In order to assess the viability (and thus the profitability) of spectrum sensing in these two cases, we would not only need to know the costs, but also the revenues which are derived from the technology. Both in case 2 and in case 3, the revenues increase if reliability of the wireless networks increases, i.e. less interference leads to more accurate machinery control in the factory. As a result, fewer production disruptions will occur and production will increase. For instance, a small increase in reliability could play an important role in detecting overheated machines. However, if networks become increasingly reliable, the added value in terms of revenues will become smaller, as the sensor network would already be accurate enough to detect machine failures.

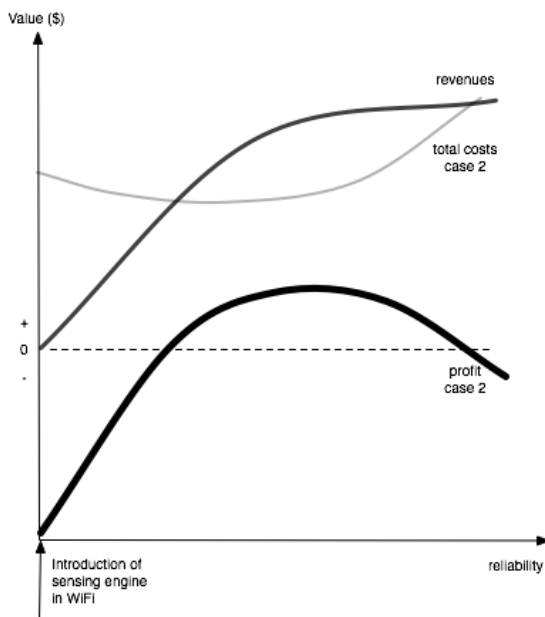


Figure 12. Case 2 - Profit curve

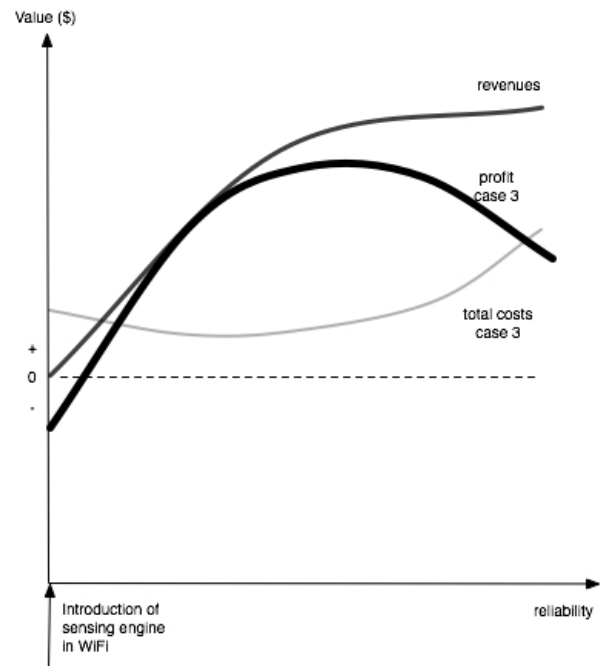


Figure 13. Case 3 - Profit curve

The depicted profit curves (Fig. 12 and 13) are the result of subtracting the total costs from the revenues, thus leaving a loss, in case the total costs surpass the revenues, or a profit, in case the revenues are larger than the total costs. As expected, the profit curve in case 3 is positive throughout, while the profit curve in case 2 starts with a serious deficit (due to the high investment and energy costs of implementing spectrum sensing engines in Zigbee nodes).

The last step in estimating the profitability of spectrum sensing is to look at the specific profit or loss that can be expected in each case, which is determined by the actual increase in reliability that can practically be achieved by spectrum sensing. As shown by the technical analysis, when spectrum sensing is deployed in the Zigbee nodes, the resulting improvement in Zigbee PER is minor; while when spectrum sensing is deployed in the WiFi nodes, the resulting improvement is dramatic. We depict these reliability points in Fig. 14, where we draw again the profit curves for cases 2 and 3, and examine the resulting profitability at these points. We conclude that the implementation of spectrum sensing in WiFi devices (case 3) is very likely to generate additional profit for the factory, compared to its current situation (case 1). Implementing spectrum sensing in the Zigbee network (case 2), however, is most likely to represent additional losses compared to the status-quo.

V. GENERAL CONCLUSIONS

In order to conclude that cognitive solutions, such as spectrum sensing, are viable, it is necessary to investigate whether it is worthwhile from an economic perspective to invest in such a technology. To do so, this paper proposes a model that derives the viability of spectrum sensing by looking at the trade-off between the increased reliability (resulting in additional revenues) of the networks involved and the additional cost, while being guided by an industrial scenario. Spectrum sensing technology would be viable in a factory setting if the economical benefit derived from the technology outweighs the additional costs. The implementation of spectrum sensing would then result in profit for the factory.

Based on techno-economic analysis, this research concludes that, from a business perspective, adding spectrum sensing to the WiFi nodes can be a viable solution in the given factory setting with coexisting 802.15.4 and 802.11 networks. Spectrum sensing technology would be viable in this case due to multiple factors. First, the total energy cost of the Zigbee sensor network is significantly decreased, as retransmissions are reduced without bearing the added energy cost of the sensing engine, and consequently the frequency of costly battery replacements is also reduced. Secondly, the investment in sensing enabled WiFi nodes would be lower than sensing enabled ZigBee nodes because of their quantity in the factory and because of the mere fact that WiFi nodes already possess some important sensing components. Lastly, the reliability of the networks would improve, with a beneficial effect on machine failure, production line efficiency, and thus revenues of the factory.

However, adding spectrum sensing to the Zigbee nodes in the factory does not make a viable case for cognitive radio networks. The business analysis shows that the high investment needed, the low energy gain and the negligible improvement in the reliability of the networks, are serious obstacles which need to be overcome in order for the solution to be profitable in a factory setting.

VI. ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Union's Seventh Framework Programme FP7/2007-2013 under grant agreements n° 257542 (CONSERN project) and n° 258301 (CREW project). It has also received funding from IWT under projects ESSENCES and NGWINETS.

REFERENCES

- [1] Healthleadersmedia (2010, 10 01), The Industry Survey [Online], Available: http://www.healthleadersmedia.com/industry_survey/index.cfm,
- [2] Cisco, the benefits of going wireless [Online], Available: <http://www.capitalnetworks.co.uk/downloads/7200%20The%20Benefits%20of%20Going%20Wireless.pdf>, 2008.
- [3] Bin Zhen, Huan-Bang Li, Shinsuke Hara, and Ryuji Kohno. 2008. Clear channel assessment in integrated medical environments. EURASIP J. Wirel. Commun. Netw. 2008, Article 48 (January 2008), 8 pages. DOI=10.1155/2008/821756 <http://dx.doi.org/10.1155/2008/821756>

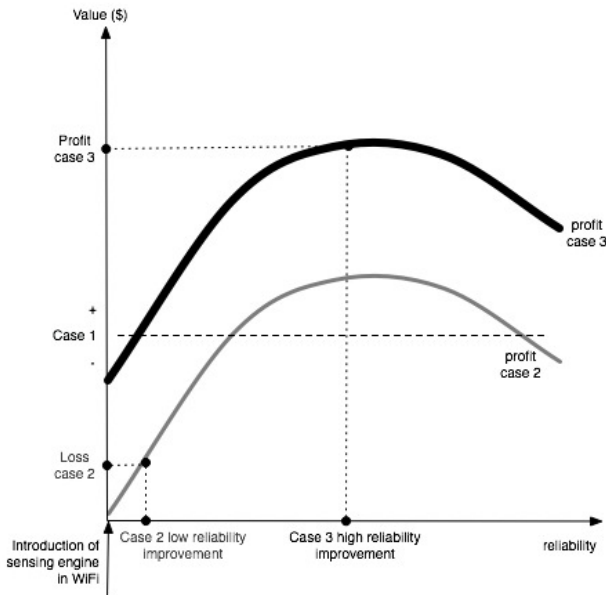


Figure 14. Profitability of case 2 and case 3

As can be seen in Fig. 14, the sensitivity of these conclusions to the actual reliability gains achieved in cases 2 and 3 is relatively low, as by the technical analysis the difference in reliability gains between cases 2 and 3 is significant. Nevertheless, sensitivity analysis of these conclusions towards different parameters, e.g. the numbers of WiFi and Zigbee nodes, remains open and is left for further research.

C. Conclusions

From a business perspective, implementing spectrum sensing in the WiFi devices can be a viable solution in the given factory setting with coexisting 802.15.4 and 802.11 networks. In this case, profit could be achieved, as well as a significant return on investment. This profitable situation is mainly a result of the high reliability improvement of the networks involved, which can only be achieved by adding sensing into the WiFi devices. Not only would all wireless networks become more robust, but it would also save on energy costs since transmissions would become more efficient. Furthermore, adding sensing in WiFi would require a smaller investment, i.e. the number of WiFi devices would typically be smaller than the number of Zigbee nodes, and the necessary additional circuitry is simpler.

The following table summarizes the results of the business analysis:

	Reliability improvement	Investment	Energy gains	Profit/loss
CASE 1	0	0	0	Status-quo
CASE 2	Low	High	Low	Loss
CASE 3	High	Medium	High	Profit

- [4] Z-Wave Alliance, WLAN Interference Raises Doubts about Zigbee, IEEE 802.15.4 Products [Online], Available: <http://electronics.ihs.com/news/zwave-zigbee-wlan.htm>, April 6, 2007.
- [5] P. Hochmuth, "Risks rise as factory nets go wireless" [Online], Available: <http://www.networkworld.com/news/2005/031405-factory-networks.html>, March 14, 2005.
- [6] I. J. Wickelgren, "Local-area networks go wireless," *IEEE Spectrum*, vol. 33, pp. 34–40, Sept. 1996.
- [7] K. Tang et al., "Wireless Communication Network Design in IC Factory", *IEEE Industrial Electronics*, Vol. 48, Nr.2, April 2001.
- [8] F. Xia et al., "Wireless Sensor/Actuator Network Design for Mobile Control Applications" *Sensors*, 2007, 7, 2157-2173
- [9] G. Garderer et al., "A novel Approach for Flexible Wireless Automation in Real-Time Environments", *WFCS*, 2008.
- [10] F. De Pellegrini et al., "On the Use of Wireless Networks at Low Level of Factory Automation Systems", *IEEE Transactions on Industrial Informatics*, May 2006.
- [11] K. M. S. J. C. Chen and P. Agrawal, "Performance comparison of battery power consumption in wireless multiple access protocols," vol. 5, pp. 445–460, 1999.
- [12] L. M. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment," in *IEEE INFOCOM*, 2001. [Online]. Available: citeseer.ist.psu.edu/feeney01investigating.html
- [13] M. Stemm and R. H. Katz, "Measuring and reducing energy consumption of network interfaces in hand-held devices," *IEICE Transactions on Communications*, vol. E80-B, no. 8, pp. 1125–1131, 1997.
- [14] M. Mathiesen et al., *Wireless AD_HOC Networks for Industrial Automation: current trends and future prospects*, ABB Corporate Research, Norway, 2005.
- [15] Jun Huang et al., "Beyond co-existence: exploiting WiFi White Space for Zigbee Performance Assurance" [online], Available: <http://www.cse.msu.edu/~huangjun/publications/icnp10.pdf>
- [16] Industrial Routing Requirements in Low-Power and Lossy Networks, rfc 5673, 2009
- [17] S. Pollin et al., "Harmful Coexistence Between 802.15.4 and 802.11: A measurement-based study," in *Proc. of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications (Crowncom)*, vol. 1, May 2008, pp. 1-6.
- [18] G. Thonet, P. Allard-Jacquín, P. Colle, "ZigBee – WiFi Coesitence White paper and Test Report" [online], Available: www.zigbee.org
- [19] M. Petrova et al., *Performance Study of IEEE 802.15.4 Using Measurements and Simulations*, WCNC 2006.
- [20] Texas Instruments (2011, 02 23), 2.4GHz IEEE 802.15.4 / Zigbee-ready RF Transceiver [online]. Available: <http://focus.ti.com/general/docs/lit/getliterature.tsp?genericPartNumber=cc2420&fileType=pdf&track=no> K.-J. Muoung, S.-Y. Shin, H.-S. Park, W.-H. Kwon, *802.11b Performance Analysis in the Presence of IEEE 802.15.4 Interference*, *IEICE Trans. Commun.*, Vol. E90-B, No.1 Jan. 2007.
- [21] IMEC (2011,02 23), IMEC sensing engine development [online], Available: <http://www.imec.be/ScientificReport/SR2008/HTML/1225000.html>
- [22] "Wireless systems for industrial automation: Process control and related applications", ISA-100.11a-2009, 2009